PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2002-252882**
(43)Date of publication of application : **06.09.2002**

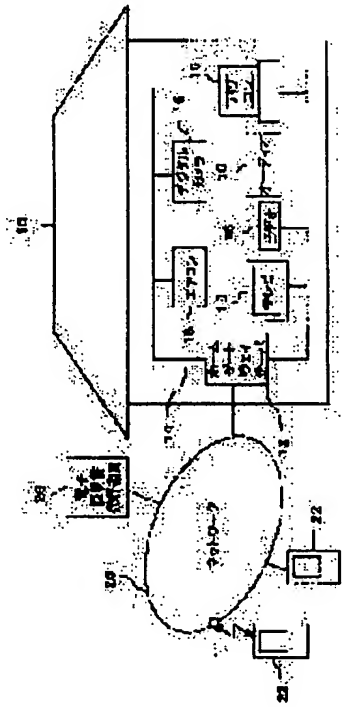
(51)Int.Cl. **H04Q 9/00**
G06F 17/60
H04M 11/00

(21)Application number : **2001-049353**
(22)Date of filing : **23.02.2001**

(71)Applicant : **SANYO ELECTRIC CO LTD**
(72)Inventor : **MATSUMOTO KENJI**

(54) REMOTE CONTROL SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To establish reliable communication between equipment outside the home and a home gateway server at home.
SOLUTION: The equipment 22 outside of the home and the home gateway server 12 are connected via a network 20. In connecting the equipment 22 and the home gateway server 12, both the equipment 22 and the home gateway server 12 are requested to show an electronic ID to the other party for authentication, preventing the occurance of wrong communication.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号
特開2002－252882
(P2002－252882A)
(43)公開日　平成14年９月６日(2002.9.6)

(51)Int.Cl.'	識別記号	FI		テーマコード'(参考)
H04Q 9/00	301	H04Q 9/00	301D	5K048
	311		311A	5K101
	321		321E	
G06F 17/60	140	G06F 17/60	140	
	176		176A	

審査請求　未請求　請求項の数６　ＯＬ　（全 5 頁）　最終頁に続く

(21)出願番号　特願2001－49353(P2001－49353)

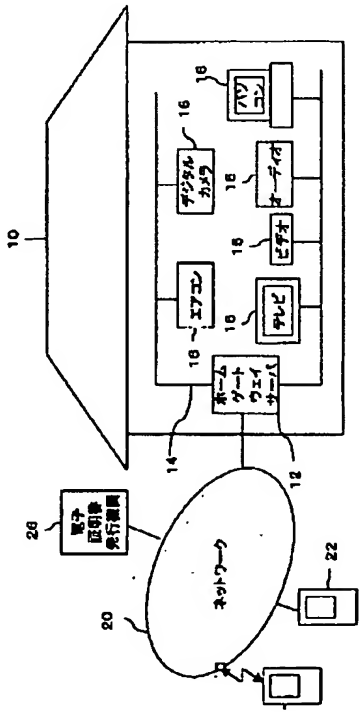
(22)出願日　平成13年２月23日(2001.2.23)

(71)出願人　000001889
三洋電機株式会社
大阪府守口市京阪本通２丁目５番５号
(72)発明者　松本　健志
大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
(74)代理人　100075258
弁理士　吉田　研二　（外２名）

Ｆターム(参考)　5K048 AA15 BA12 BA13 BA53 DC07
EB02 HA01 HA02
5K101 KK11 LL01

(54)【発明の名称】　リモート操作システム

(57)【要約】
【課題】　宅外機器と宅内のホームゲートウェイサーバとの通信を確実なものにする。
【解決手段】　宅外機器２２とホームゲートウェイサーバ１２をネットワーク２０を介し接続する。そして、この接続に対し、宅外機器２２とホームゲートウェイサーバ１２の両者において相手方に電子証明書の提示を求め認証を行う。そこで、誤った通信の発生を確実に防止することができる。



1

【特許請求の範囲】

【請求項１】　ホストに接続された電気機器を携帯機器から通信を利用して制御するリモート操作システムであって、

携帯機器とホストの両方において相手側を認証し、認証に成功したときに携帯機器による前記電気機器の操作を許可するリモート操作システム。

【請求項２】　請求項１に記載のシステムにおいて、

前記ホストは家庭に置かれるコンピュータであり、前記電気機器は家庭に置かれる複数の電気機器であるリモート操作システム。

【請求項３】　請求項１に記載のシステムにおいて、

前記ホストは家庭に置かれる電気機器であるリモート操作システム。

【請求項４】　請求項１～３のいずれか１つに記載のシステムにおいて、

前記ホストと、携帯機器とを直接接続し、認証のためのデータを交換するリモート操作システム。

【請求項５】　電気機器を携帯機器から通信を利用して制御するリモート操作システムであって、

前記電気機器と携帯機器の両方において相手側を認証し、認証に成功したときに携帯機器による前記電気機器の操作を許可するリモート操作システム。

【請求項６】　請求項１～５のいずれか１つに記載のシステムにおいて、

前記認証は、第三者機関の発行した電子証明書を利用するリモート操作システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ホストに接続された電気機器を携帯機器から通信を利用して制御するリモート操作システムに関する。

【０００２】

【従来の技術】従来より、電話等によって、家庭内機器（エアコンやビデオデッキ等）を制御するシステムがある。このようなシステムによれば、帰宅前にエアコンのスイッチを入れたり、外からビデオの予約ができる。

【０００３】しかし、電話機による操作では、操作者の特定は暗証番号の入力などによる他になく、セキュリティ管理が十分でないという問題がある。また、暗証番号の入力もない場合には、誤って電話を掛けた相手に偶然同じ設備があった場合に、これを誤って操作してしまう可能性もある。

【０００４】そこで、特開平１０－２８９２０５号公報には、電子メールによって、機器制御を行うシステムが提案されている。このシステムでは、認証情報付きの電子メールを送信するため、家庭側システムにおいて、メール送信者を認証することができる。従って、不審者によるアクセスなどを防止することができる。

2

【発明が解決しようとする課題】しかし、上記従来システムにおいては、認証付きの電子メールを誤ったアドレスに送信してしまった場合にこれが受信され、これに基づいてなりすましされる危険がある。また、宅外の携帯端末がメール送受信機能を有するものに限定されるという問題があった。さらに、制御の際にメール送信の作業が必要であり、メール送信についての知識も必要であるという問題があった。

【０００６】本発明は、上記課題に鑑みなされたものであり、セキュリティ性が向上でき、かつ操作が容易なリモート操作システムを提供することを目的とする。

【０００７】

【課題を解決するための手段】本発明は、ホストに接続された電気機器を携帯機器から通信を利用して制御するリモート操作システムであって、携帯機器とホストの両方において相手側を認証し、認証に成功したときに携帯機器による前記電気機器の操作を許可することを特徴とする。

【０００８】このように、本発明によれば、携帯機器と、ホストの両方において、相手側を認証する。従って、一方的な認証と異なり、誤った接続により通信が行われしまうことを防止することができる。

【０００９】また、前記ホストは家庭に置かれるコンピュータであり、前記電気機器は家庭に置かれる複数の電気機器であることが好適である。これによって、家庭内の電気機器を宅外から、確実に操作できる。

【００１０】また、前記ホストは家庭に置かれる電気機器であることも好適である。電気機器がホストとして機能することで、独立したコンピュータを不要にできる。

【００１１】また、前記ホストと、携帯機器とを直接接続し、認証のためのデータを交換することが好適である。携帯機器を宅外に持ち出すときなどに、接続してデータ交換を行うことで、携帯機器における処理負荷を低減できる。

【００１２】さらに、本発明は、電気機器を携帯機器から通信を利用して制御するリモート操作システムであって、前記電気機器と携帯機器の両方において相手側を認証し、認証に成功したときに携帯機器による前記電気機器の操作を許可することを特徴とする。このシステムによっても、電気機器を携帯機器で確実に制御することができる。

【００１３】また、前記認証は、第三者機関の発行した電子証明書を利用することが好適である。第三者機関を利用することによって、より確実な認証が行える。

【００１４】

【発明の実施の形態】以下、本発明の実施形態について、図面に基づいて説明する。

【００１５】図１は、実施形態のシステムの全体構成を示す図である。家庭（自宅）１０には、ホームゲートウ

ェイサーバ１２にホームネットワーク１４が接続されている。そして、このホームネットワークにエアコン、デジタルカメラ、テレビ、ビデオ、オーディオ、パソコン（パーソナルコンピュータ）などの各種電気機器１６が接続されている。このホームネットワーク１２は、各種電気機器１６と通信が行え、これらについて必要な制御が行えれば、独自のプロトコルで接続してもよいが、外部との通信と同様にインターネットプロトコルで接続してもよい。また、接続は、無線で行ってもよい。

【００１６】ホームゲートウェイサーバ１２には、ネットワーク２０が接続されている。このネットワークは例えばインターネットであり、ホームゲートウェイサーバ１２がインターネットを介しての通信を行う。

【００１７】ホームゲートウェイサーバ１２は、図２に示すように、家庭内機器情報１２ａと、自己の電子証明書１２ｂ、宅外機器情報１２ｃを有しており、通信や制御の際にこれら情報を利用する。家庭内機器情報１２ａは、接続機器リスト、接続機器のオンオフ情報、機器毎の操作についての操作情報、誰にアクセスを許可するかという許アクセス権情報などがある。また、宅外機器情報１２ｃには、登録されている宅外機器についての情報である登録機器リスト、電子証明書についての発行リストおよび無効リスト情報、各宅外機器２２についてのどのようなアクセスを許可するかについてのアクセス権情報などがある。

【００１８】ネットワーク２０には、宅外機器２２が接続されている。この宅外機器２２は、ウェッブブラウザを搭載しており、インターネットを介して各種のウェッブページにアクセス可能になっている。宅外機器２２は、携帯電話機やＰＤＡ（パーソナル・デジタル・アシスタント）等であるが、パソコンでもよい。さらに、携帯可能な宅外機器２２の他に、デスクトップ型など据え置き型のパソコンを併せて利用することもできる。

【００１９】さらに、ネットワーク２０には、電子証明書発行機関２６が接続されている。この電子証明書発行機関２６は、セキュリティの確保のために、通信相手の要求に対して電子証明書を発行する機関である。電子証明書は、例えばＸ．５０９として規格化されているもの等が利用でき、証明書発行機関の署名、暗号化キー（鍵）、証明書期限などが記載されている。

【００２０】ホームゲートウェイサーバ１２、宅外機器２２は、それぞれ電子証明書発行機関２６から電子証明書を発行してもらい、これ利用して相互に認証を行う。

【００２１】ここで、ゲートウェイサーバ１２は、ホームネットワーク１４に接続されている電気機器１６の情報を管理し、外部からの閲覧を可能とする。例えば、ホームページ上に情報を置くことによって宅外機器２２からブラウザを用いてアクセス（閲覧）可能にする。すなわち、宅外機器２２は、ブラウザ機能によって、ホーム１６についての情報を入手したり、操作の指示を行う。

【００２２】また、このアクセスにおいて、電子証明書発行機関２６の発行する電子証明書を利用したセキュア通信プロトコルを利用する。このセキュア通信プロトコルとしては、例えばＳＳＬ（Secure Sockets Layer）が利用される。また、宅外機器２２のブラウザにＳＳＬを組み込んでおくことで、使用者は煩わしい操作の必要がなく、ＳＳＬを利用することができる。

【００２３】そして、本実施形態においては、相互認証方式を採用している。これについて、図３に基づいて説明する。図３は、宅外機器２２からのアクセスがあった場合を示している。まず、宅外機器２２によりインターネットを介し、ホームゲートウェイサーバ１２にアクセスする。そして、（ｉ）最初に宅外機器２２がホームゲートウェイサーバ１２に対し証明書提示を要求する。（ｉｉ）ホームゲートウェイサーバ１２は、予め取得してある証明書を提示する。（ｉｉｉ）宅外機器２２は受け取った証明書を確認し、ホームゲートウェイサーバ１２を認証する。（ｉｖ）一方、証明書を提示したホームゲートウェイサーバ１２は、宅外機器２２に対し、証明書の提示を要求する。（ｖ）ホームゲートウェイサーバ１２を認証した宅外機器２２は要求に応じて自己の証明書を提示する。（ｖｉ）ホームゲートウェイサーバ１２は、送られてきた宅外機器２２の証明書を確認し、宅外機器２２を認証する。

【００２４】このようにして、相手を相互に認証できた場合には、（ｖｉｉ）共通鍵暗号方式の暗号化キー（共通キー）を交換し、（ｖｉｉｉ）その後のやりとりは、暗号化した通信により行う。

【００２５】なお、図３では、ホームゲートウェイサーバ１２が暗号化キーを作成し宅外機器２２に渡しているが、これには限られず、宅外機器２２が暗号化キーを作成してホームゲートウェイサーバ１２に渡すことで暗号化キーの交換を行ってもよい。

【００２６】また、上述の例では、宅外機器２２が単独で、電子証明書発行機関２６から証明書の発行を受けた。しかし、携帯用の宅外機器２２は、必要なときに宅外に持ち出すもので、在宅時には宅内にある。そこで、宅外機器２２を宅内においてホームネットワーク１４に接続するなどの手段で、ホームゲートウェイサーバ１２に接続して、電子証明書発行機関２６に登録するとともに、電子証明書の発行を受けることもできる。また、この際にホームゲートウェイサーバ１２の証明書情報（公開鍵など）も入手する。

【００２７】また、宅外機器２２において、ホームゲートウェイサーバ１２との通信に必要なアプリケーションプログラムをダウンロードしておくことも好適である。

【００２８】そして、宅外機器２２は、宅外からホームゲートウェイサーバ１２にアクセスしたときには、ホー

5

外機器２２が宅内において取得したホームゲートウェイサーバ１２の証明書情報と一致しているかを照合する。あるいは、宅外機器２２内に取得しているホームゲートウェイサーバ１２の公開鍵で、証明書を復号することで認証してもよい。

【００２９】このように、本システムでは、宅外機器２２は、外出するときに持ち出すもので、その使用者は自宅１０に戻ってくることが前提となっている。このため、宅外機器２２とホームゲートウェイサーバ１２との一対一の証明書発行作業が行える。これによって、宅外機器２２は、独自に電子証明書発行機関にアクセスし、証明書を取得するなどの作業が不要になり、宅外機器２２の負荷を軽くすることができる。

【００３０】例えば宅外機器２２に電子キーとしての機能を持たせ、玄関をでるときに、この携帯端末を所定の位置にセットすることで、玄関をロックする。このときに、ホームネットワーク１４に接続し、上述のような証明書情報を入手することが好ましい。

【００３１】また、宅外機器２２を宅外で紛失等した場合、ホームゲートウェイサーバ１２において、その宅外機器２２の持っている電子証明書情報を電子証明書無効リストに載せることで、紛失した宅外機器２２からの他人による不正アクセスを防止することができる。

【００３２】ホームゲートウェイサーバ１２においては、宅外機器２２から送られた電子証明書が正しい証明書であること、証明期限が切れていないことなどから携帯機器２２を認証し、アクセスを許可する。

【００３３】なお、外部の電子証明書発行機関２６を利用することなく、ホームゲートウェイサーバ１２が独自に電子証明書を発行し、これを利用して相互の認証を行ってもよい。

【００３４】また、宅外機器２２からのアクセスについては、その範囲を設定できるようにすることも好適である。ホームゲートウェイサーバ１２に宅外機器２２を登録し、その宅外機器２２に許可するアクセスの範囲を設定しておく。すなわち、ホームネットワーク１４に接続されている電気機器１６の内のどの電気機器１６についてどのような操作を許可するか、どの情報についてホームゲートウェイサーバ１２から取り出すことを許可するかなどを設定しおく。そして、宅外機器２２からのアクセスについては、設定されているものだけに限定する。これによって、子供の所有する宅外機器２２についてアクセス可能機器を制限するなどの設定が可能になる。

6

【００３５】また、アクセス権をホームゲートウェイサーバ１２が発行する電子証明書内に記載しておいてもよい。

【００３６】また、宅外機器２２とホームゲートウェイサーバ１２とを無線で接続し、宅外機器２２がホームゲートウェイサーバ１２から所定の通信可能範囲内にいるときには、宅外機器２２はホームゲートウェイサーバ１２と直接接続し、通信不能範囲に至ったときに、上述のようなネットワーク２０を介した通信に移ることも好適である。

【００３７】ホームゲートウェイサーバ１２は、家庭内に置かれるコンピュータである他、冷蔵庫のような常時電源を立ち上げている機器や、テレビ、ビデオなどの高機能なＣＰＵを搭載した電気機器にハードディスクなどの記憶装置を備えても本発明を実現することが可能である。

【００３８】さらに、ホームネットワーク１４に接続された電気機器１６がそれぞれ電子証明書を持ち、宅外機器２２は各電気機器１６と個別に認証を行い、アクセス許可を得て、電気機器１６の操作を行うことも可能である。

【００３９】

【発明の効果】以上説明したように、本発明によれば、携帯機器と、ホストの両方において、相手側を認証する。従って、一方的な認証と異なり、誤った接続により通信が行われしまうことを防止することができる。特に、宅外から自宅の電気機器などを確実に操作できる。また、携帯機器とホストを接続して、データ交換を行うことで、携帯機器における処理負荷を低減できる。また、第二者機関の認証を利用することによって、より確実な認証が行える。

【図面の簡単な説明】

【図１】　システムの全体構成を示す図である。

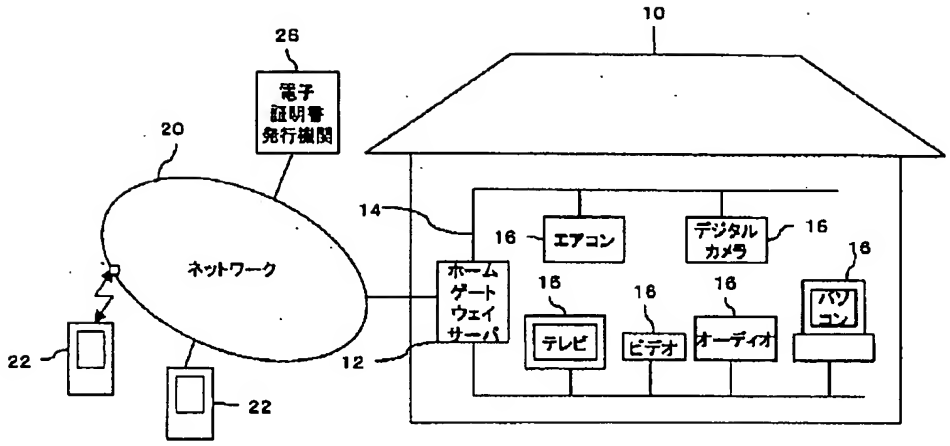
【図２】　ホームゲートウェイサーバの所有する情報を示す図である。

【図３】　通信の手順を示す図である。

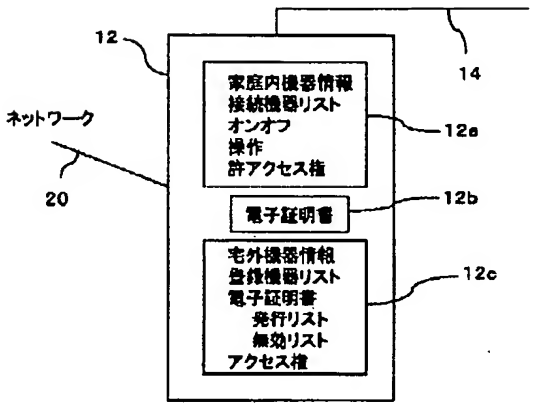
【符号の説明】

１０　自宅、１２　ホームゲートウェイサーバ、１４　ホームネットワーク、１６　電気機器、２０ネットワーク、２２　宅外機器、２６　電子証明書発行機関。

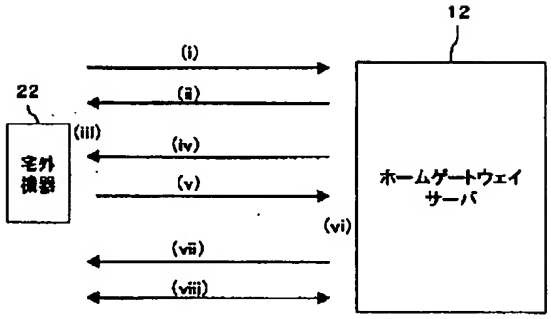
【図１】



【図２】



【図３】



フロントページの続き

(51) Int. Cl.[7]	識別記号	F I		ﾃｰﾏｺｰﾄﾞ（参考）
Ｇ０６Ｆ　17/60	５０６	Ｇ０６Ｆ　17/60	５０６	
Ｈ０４Ｍ　11/00	３０１	Ｈ０４Ｍ　11/00	３０１	